

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-134260

(43)Date of publication of application : 20.05.1997

(51)Int.Cl.

G06F 3/06
G06F 9/06

(21)Application number : 07-288932

(71)Applicant : FUJITSU LTD

(22)Date of filing : 07.11.1995

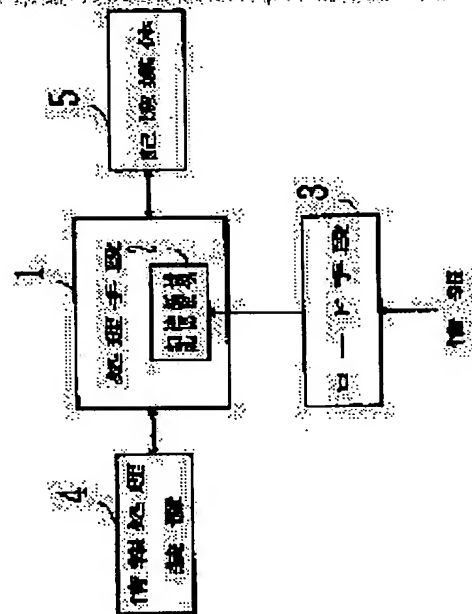
(72)Inventor : KOTANI MASATAKE
MURAKAMI KEIICHI
YOSHIMOTO SHINICHI
KANEMOTO KOICHI
MASUDA TATSURO
YOSHIOKA MAKOTO
FUJIWARA MASAO

(54) MEDIUM CONTROL METHOD AND DEVICE HAVING SECURITY FUNCTION

(57)Abstract:

PROBLEM TO BE SOLVED: To attain the loading of a processing program and to flexibly protect the security of information stored in a loaded medium by adding a rewritable area to the processing part of an external storage.

SOLUTION: A medium controller is provided with a processing means 1 and a loading means 3 and contained in an external storage. Then the medium controller performs the processing concerning the transfer of data between an information processor 4 and a storage medium 5. The medium 1 has a rewritable storage means 2 and performs the processing concerning the protection of the storage contents of the medium 5 based on the information stored in the area 2. The means 3 loads the information into the area 2 of the means 1. Thus the processing program to be carried out by the means 1 can be loaded and the storage contents of the medium 5 can be flexibly protected owing to the presence of the area 2 and the means 3 of the medium controller.



LEGAL STATUS

[Date of request for examination]

24.03.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-134260

(43) 公開日 平成9年(1997)5月20日

(51) Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 3/06	3 0 4		G 0 6 F 3/06	3 0 4 H
9/06	5 5 0		9/06	5 5 0 X

審査請求 未請求 請求項の数15 O L (全 12 頁)

(21) 出願番号 特願平7-288932

(22) 出願日 平成7年(1995)11月7日

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72) 発明者 小谷 誠剛

神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72) 発明者 村上 敬一

神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(74) 代理人 弁理士 大菅 義之 (外1名)

最終頁に続く

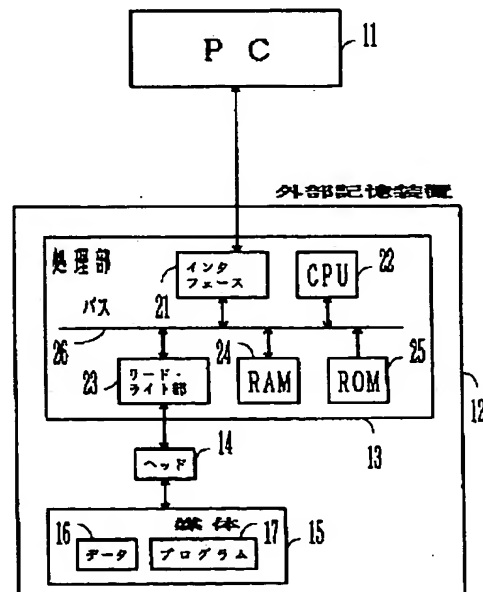
(54) 【発明の名称】 セキュリティ機能を有する媒体制御装置および方法

(57) 【要約】

【課題】 取り外し可能な記憶媒体への不正なアクセスをリーズナブルなコストで防止することを課題とする。

【解決手段】 外部記憶装置12の処理部13はRAM(ランダムアクセス・メモリ)24を備え、その内容はロードابلである。CPU(中央処理装置)22は、インタフェース21やリード・ライト部23を介してRAM24にロードされたプログラムを用いて、PC(パーソナル・コンピュータ)11と媒体15間のデータの授受に関する処理を行う。そして、媒体15へのアクセスの可否を判定したり、暗号化されたデータ17を復号したりする。RAM24の内容を書き換えることにより、フレキシブルで効率的な記憶内容の保護が実現される。

実施形態の構成図



【特許請求の範囲】

【請求項1】 取り外し可能な記憶媒体と組み合わせて使用され、該記憶媒体の記憶内容に関する処理を行う外部記憶装置において、

書き換え可能な記憶領域を有し、該記憶領域に格納された情報を利用して、前記記憶媒体の記憶内容の保護に関する処理を行う処理手段と、

前記記憶領域に前記情報をロードするロード手段とを備えることを特徴とする媒体制御装置。

【請求項2】 前記処理手段は、前記記憶領域にアクセス判定アルゴリズムを記憶し、該判定アルゴリズムを用いて、前記外部記憶装置が前記記憶媒体にアクセス可能か否かの判定を行うことを特徴とする請求項1記載の媒体制御装置。

【請求項3】 前記記憶媒体がロード可能なプログラムを搭載しているとき、前記ロード手段は該プログラムを前記記憶領域にロードし、前記処理手段は該プログラムを用いて該記憶媒体内のデータへのアクセスに関する処理を行うことを特徴とする請求項1記載の媒体制御装置。

【請求項4】 前記処理手段は、前記記憶媒体内に保持されたメディア識別記号を用いて、前記外部記憶装置が該記憶媒体にアクセス可能か否かのアクセス判定を行うことを特徴とする請求項1記載の媒体制御装置。

【請求項5】 取り外し可能な記憶媒体と組み合わせて使用され、該記憶媒体の記憶内容に関する処理を行う外部記憶装置において、

前記記憶媒体内に保持されたメディア識別記号および許諾記号を読み出すリード手段と、

該メディア識別記号を用いて判定記号を作成し、該判定記号を前記許諾記号と比較して、前記外部記憶装置が該記憶媒体にアクセス可能か否かのアクセス判定を行う処理手段とを備えることを特徴とする媒体制御装置。

【請求項6】 前記処理手段は、前記判定記号が前記許諾記号と一致した場合に、アクセス可能であると判定することを特徴とする請求項5記載の媒体制御装置。

【請求項7】 前記処理手段は、前記外部記憶装置内に保持された装置識別記号を読み出し、前記メディア識別記号および該装置識別記号を用いて前記判定記号を作成することを特徴とする請求項5記載の媒体制御装置。

【請求項8】 前記判定記号が前記許諾記号と一致しなかった場合、前記処理手段は、前記メディア識別記号を用いて所定の記号を作成し、該所定の記号を前記許諾記号と比較し、該所定の記号と前記許諾記号が一致すれば前記記憶媒体内の該許諾記号を前記判定記号に置き換えて、置き換えられた許諾記号を該判定記号と比較することにより、前記アクセス判定を行うことを特徴とする請求項5記載の媒体制御装置。

【請求項9】 前記処理手段は、前記所定の記号として、前記記憶媒体の供給者が該記憶媒体内に前記許諾記

号として設定した供給者保証記号を作成することを特徴とする請求項8記載の媒体制御装置。

【請求項10】 前記処理手段は、前記所定の記号として、前記記憶媒体のユーザが該記憶媒体内に前記許諾記号として設定した特殊記号を作成することを特徴とする請求項8記載の媒体制御装置。

【請求項11】 前記処理手段は、前記所定の記号と前記許諾記号が一致しなかった場合に、アクセス不可能であると判定することを特徴とする請求項8記載の媒体制御装置。

【請求項12】 前記処理手段は、前記記憶媒体内に保持された複数の許諾記号を順に前記所定の記号と比較し、該所定の記号と一致した許諾記号を前記判定記号に置き換えて、置き換えられた許諾記号を該判定記号と比較することにより、前記アクセス判定を行うことを特徴とする請求項8記載の媒体制御装置。

【請求項13】 取り外し可能な記憶媒体と組み合わせて使用され、該記憶媒体の記憶内容に関する処理を行う外部記憶装置であって、

書き換え可能な記憶領域を有し、該記憶領域に格納された情報を利用して、前記記憶媒体の記憶内容の保護に関する処理を行う処理手段と、

前記記憶領域に前記情報をロードするロード手段とを備えることを特徴とする外部記憶装置。

【請求項14】 外部記憶装置に装着されて使用される取り外し可能な記憶媒体であって、

メディア識別記号を保持するメディア識別記号領域手段と、

前記外部記憶装置が前記記憶媒体にアクセス可能か否かを判定するアクセス判定において、前記メディア識別記号を用いて作成される判定記号と比較される許諾記号を保持する許諾記号領域手段とを備えることを特徴とする記憶媒体。

【請求項15】 外部記憶装置内の書き換え可能な記憶領域に情報をロードし、

該記憶領域にロードされた該情報を利用して、前記外部記憶装置に装着された記憶媒体の記憶内容の保護に関する処理を行うことを特徴とする媒体制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は取り外し可能な記憶媒体に係り、その記憶内容のセキュリティを保つ機能を持つ媒体制御装置およびセキュリティを保証する記憶媒体の制御方法に関する。

【0002】

【従来の技術】情報処理技術の分野において、情報を記録する記憶媒体にはいくつかの種類のものがある。従来より用いられている取り外し可能な記憶媒体としては、磁気テープ、磁気ディスク、光磁気ディスク、光ディスク等が知られており、今日ではますます多様化する傾向

にある。

【0003】近年、このような可搬性のある記憶媒体の大容量化によって、大量の情報を収納、供給、分配することが可能となってきた。これに伴い、記憶された情報のセキュリティをどのように保証するか、あるいは記憶された著作物の著作権の保護をどのように保証するかについて、関心が高まっている。

【0004】情報のセキュリティや著作権の保護等は、情報の完全な囲い込みによって達成可能である。しかしながら、情報を完全に囲い込むシステムを構築するには、多大なコストを要する。また、取り外し可能な記憶媒体に対して、紛失、盗難等の危険性を零にすることは事実上不可能である。

【0005】

【発明が解決しようとする課題】従来の可搬性記憶媒体内の情報のセキュリティ保護に関しては、次のような問題がある。

【0006】取り外し可能な記憶媒体が、過失あるいは不正な手段等により、他の悪意ある人々の手に渡るのを完全に封じることが不可能である。記憶媒体が何等かのルートで悪意ある人の手に渡った場合、その媒体内の情報に対してその人がアクセス可能であるならば、その情報のセキュリティや著作権の保護等は保証されない。したがって、そのような事態において、媒体内の情報への不正なアクセスを不可能にすることが望まれる。

【0007】本発明は、取り外し可能な記憶媒体への不正なアクセスをリーズナブルなコストで防止できる媒体制御装置およびその方法を提供することを目的とする。

【0008】

【課題を解決するための手段】図1は、本発明の媒体制御装置の原理図である。図1の媒体制御装置は処理手段1とロード手段3を備え、外部記憶装置内に設けられる。そして、情報処理装置4と記憶媒体5の間のデータのやり取りに関する処理を行う。

【0009】処理手段1は書き換え可能な記憶領域2を有し、その記憶領域2に格納された情報を利用して、記憶媒体5の記憶内容の保護に関する処理を行う。ロード手段3は、処理手段1の記憶領域2に上記情報をロードする。

【0010】このように、媒体制御装置に書き換え可能な記憶領域2とロード手段3とを設けたことで、処理手段1が実行する処理プログラムがロード可能になり、記憶媒体5の記憶内容の保護をフレキシブルに行うことができる。

【0011】例えば、ロード手段3がデータと対して記憶媒体5内に記憶されたプログラムをロードし、処理手段1がそのプログラムを用いてデータへのアクセスに関する処理を行う。これにより、データ毎にまたは媒体毎に異なるアクセスアルゴリズムや暗号化アルゴリズムを採用することが可能になる。

【0012】また、処理手段1は、記憶領域2にアクセス判定アルゴリズムを記憶し、それを用いて、外部記憶装置が記憶媒体5にアクセス可能か否かの判定を行う。判定アルゴリズムの一例として、記憶媒体5とその記憶内容にアクセスできる外部記憶装置とを対にすることをある段階で許諾し、それ以外の組合せにおいては媒体へのアクセスを禁止する方法を用いる。

【0013】この方法によれば、許諾された記憶媒体と外部記憶装置の対においてのみ、記憶内容へのアクセスが許可される。このため、過失や故意によって他の対が形成された場合に、アクセスを禁止することができ、記憶内容のセキュリティや著作権の保護等が保証される。

【0014】例えば、図1の処理手段1は実施形態における図2の処理部13に対応し、記憶領域2はRAM（ランダムアクセス・メモリ）24に対応し、ロード手段3はインタフェース21またはリード・ライト部23に対応する。また、情報処理装置4は、例えばパーソナルコンピュータ（PC）11に対応する。

【0015】

【発明の実施の形態】以下、図面を参照しながら本発明の実施の形態を詳細に説明する。図2は、実施形態の情報処理システムの構成図である。図2の情報処理システムは、PC11と外部記憶装置12を備える。

【0016】外部記憶装置12は、装着された媒体15へのアクセスを行うヘッド14と、それを制御するためのドライブ処理を行う処理部13を備え、PC11からの指示等に基づいて媒体15の記憶内容をアクセスする。媒体15には、例えば、データ16とロード可能なプログラム17が格納されている。プログラム17は、例えば、データ16をアクセスするために必要なアルゴリズムを含み、データ16が暗号化されている場合は、さらにその復号アルゴリズムも含む。

【0017】処理部13は、インタフェース21、CPU（中央処理装置）22、リード・ライト部23、RAM24、ROM（リードオンリー・メモリ）25、およびそれらを結合するバス26を備え、PC11と通信しながら媒体15へのアクセス処理を行う。

【0018】インタフェース21はPC11との間で情報のやり取りを行い、リード・ライト部23はヘッド14を制御して、媒体15の記憶内容を読み出したり、媒体15への書き込みを行ったりする。CPU22は、RAM24やROM25内の情報を用いてドライブ処理を行う。例えば、CPU22としてはマイクロ・プロセッサが用いられ、処理部13はマイクロ・コンピュータとして構成される。

【0019】ROM25には、外部記憶装置12の電源投入（パワーオン）時に実行されるドライブ処理のプログラムがあらかじめ格納されている。また、RAM24には、外部記憶装置12が媒体15にアクセス可能か否かの判断を行うプログラムが格納され、CPU22はそ

のアルゴリズムを用いてアクセス判定を行う。RAM 24 内のプログラムがデータ 16 の復号アルゴリズムを含む場合は、CPU 22 はそれを用いてデータ 16 を復号する。

【0020】RAM 24 内のプログラムは、インタフェース 21 やリード・ライト部 23 を介してロードした情報を用いて書き換えることができ、そのアルゴリズムは可変（ロードブル）である。処理部 13 へのプログラムのローディング方法としては、例えば、媒体 18 や PC 11 からロードして RAM 24 に格納する方法がある。そのほかにも、ROM 25 にプログラムを書き込んでおき、変更時には ROM 25 ごと交換するなど、種々の方法が考えられる。

【0021】次に、図 3 から図 5 までを参照しながら、データ 16 が暗号化されている場合に、それを読み出して復号するドライブ処理について説明する。図 3 は、処理部 13 の動作フローチャートである。図 3 において、外部記憶装置 12 に電源が投入されると（ステップ S 1）、CPU 22 は、ROM 25 内のプログラムによるドライブ処理を行い（ステップ S 2）、電源がオフになると（ステップ S 3）、処理を終了する。

【0022】図 4 は、図 3 のステップ S 2 で行われる媒体判別処理のフローチャートである。図 4 において処理が開始されると、処理部 13 は、ヘッダ 14 からの情報を元に外部記憶装置 12 に媒体 15 がセットされたかどうかを判定する（ステップ S 11）。媒体 15 がセットされていなければこの判定を繰り返し、媒体 15 がセットされれば、その所定領域のデータを読み取る（ステップ S 12）。

【0023】そして、媒体 15 がロード可能（ロードブル）なプログラムを搭載していることを、そのデータが示しているかどうかを判定する（ステップ S 13）。読み取ったデータがロードブルなプログラムの搭載を示していれば、媒体 15 からそのプログラム 17 を読み出して RAM 24 に格納し（ステップ S 14）、そのプログラム 17 に基づく復号処理を行って（ステップ S 15）、処理を終了する。

【0024】また、媒体 15 がロードブルなプログラムを搭載していないと判定されれば、あらかじめ RAM 24 に格納されていたプログラムに基づく復号処理を行って（ステップ S 15）、処理を終了する。

【0025】図 5 は、図 4 のステップ S 15 で行われるデータ 16 の復号処理のフローチャートである。図 5 において処理が開始されると、処理部 13 は、まず PC 11 からデータ 17 のリード要求とともに暗号解読用のキーを受け取る（ステップ S 21）。

【0026】次に、媒体 15 中の暗号化されたデータ 16 を読み出し（ステップ S 22）、RAM 24 内のプログラム 17 のアルゴリズムに従い、キーを用いてデータ 16 を復号する（ステップ S 23）。このとき、例え

ば、プログラム 17 に定められた変換式中の変数にキーを代入して、データ 16 の変換を行う。そして、復号されたデータを PC 11 に渡して（ステップ S 24）、処理を終了する。

【0027】このように、データ 16 と対にして格納されたプログラム 17 を用いて復号処理を行うことで、データ毎または媒体毎に異なる復号アルゴリズムを用いることができるようになる。

【0028】次に、図 6 から図 11 までを参照しながら、処理部 13 による装着媒体へのアクセス判定処理について説明する。図 6 は、アクセス判定を行う場合の情報処理システムの構成図である。図 6 において、基本的に図 2 と同様の構成要素には同じ符号が付けられている。PC 11 は、ユーザのアプリケーション・プログラム 31 と、外部記憶装置 12 にアクセスするためのソフトウェアツールであるデバイスドライバ 32 を有する。また、外部記憶装置 12 の処理部 13 は、ドライブ識別記号（DID: drive identifier）を記憶する DID 記憶部 33 を備える。

【0029】DID は、外部記憶装置 12 のドライブをユニークに限定することのできる装置識別記号であり、例えば外部記憶装置 12 の製造時のシリアル番号、またはこれに類する記号等が用いられる。この DID は書き換え不可能であることが望ましく、DID 記憶部 33 は、例えば ROM 25 内に設けられる。

【0030】媒体 34 内には、メディア識別記号（MID: medium identifier）を記憶する MID 領域 35 と、許諾記号（LC: license code）を記憶する LC 領域 36 が設けられる。

【0031】MID は、媒体 34 をユニークに限定することのできる識別子であり、書き換え不可能な方法で媒体に書き込まれることが望ましい。このため、MID 領域 35 は、媒体 34 内の書き換え不可能な部分に設けられる。そのほかにも、例えば論理的パリティチェックを多用して記号構造を複雑にするなど、書き換えに多大のコストを要する方法を用いて、MID を書き込んでもよい。

【0032】また、LC 領域 36 は媒体 34 内の書き換え可能な部分に設けられ、処理部 13 が媒体 34 へのアクセスの可否を判定する際に用いられる。処理部 13 は、アクセス判定において、必要に応じて LC を書き換えることができる。ただし、PC 11 内のアプリケーション・プログラム 31 やデバイスドライバ 32 は、この LC 領域 36 にアクセスすることはできない。

【0033】以下の実施形態で用いる判定アルゴリズムによれば、媒体 34 とその記憶内容にアクセスできる外部記憶装置 12 とを対にすることをある段階で許諾し、それ以外の組合せにおいては媒体へのアクセスができないようにする。そのために、処理部 13 は媒体 34 上の MID と外部記憶装置 12 上の DID からユニークに決

められる判定記号(JC: judge code)を生成する。そして、LCとJCを用いてアクセス判定を行う。

【0034】図7は、処理部13による第1のアクセス判定処理のフローチャートである。図7において処理が開始されると、処理部13は、まずDID記憶部33からDIDを読み出し(ステップS31)、媒体34からMIDとLCを読み出す(ステップS2)。そして、第1の記号生成アルゴリズムに従ってMIDとDIDからJCを作成し(ステップS33)、それをLCと比較する(ステップS34)。作成したJCが媒体34のLCと一致すれば、外部記憶装置12による媒体34へのアクセスが可能と判定し(ステップS35)、処理を終了する。

【0035】これ以降は、PC11からの要求に従って、媒体34にアクセスすることが可能になる。ステップS34においてJCがLCと一致しなかった場合は、次に、第2の記号生成アルゴリズムに従ってMIDから供給者保証記号(SGC: supplier guarantee code)を作成し(ステップS36)、それをLCと比較する(ステップS37)。

【0036】SGCは、媒体34の出荷時に、その供給者により上記第2の記号生成アルゴリズムと同じアルゴリズムに従って生成され、媒体34のLC領域36にLCの初期値として書き込まれている。処理部13は、そのSGCを作成して媒体34上のLCと比較することにより、媒体34のLCが出荷時のままであるかどうかを調べることができる。

【0037】ここで、作成したSGCがLCと一致すれば媒体34はまだ新しいことが分かるので、媒体34上のLCをJCに置き換え(ステップS38)、ステップS32以降の処理を繰り返す。この場合、LC領域36内のLCはJCそのものであるので、ステップS34においてLCとJCが一致し、アクセスが可能になる(ステップS35)。

【0038】一方、SGCとLCが一致しなかった場合は、外部記憶装置12による媒体34へのアクセスは不可能と判定し(ステップS39)、処理を終了する。この場合には、LC領域36にSGCやJC以外の記号、例えば他の記号生成アルゴリズムや他の装置のDIDを用いて生成されたJCが書き込まれており、外部記憶装置12の媒体34へのアクセスが禁止される。

【0039】このように、MIDとDIDの両方を用いてJCを作成し、それをLC領域36に書き込むことにより、他のDIDを持つ装置による媒体34へのアクセスを禁止することができる。言い換えれば、媒体34にアクセス可能な外部記憶装置12がLC領域36に登録されることになる。

【0040】尚、ステップS33において、MIDのみを用いてJCを作成することにしてもよい。その場合も、他のシステムと異なる生成アルゴリズムでJCを作

成すれば、同様の効果を得ることができる。

【0041】以上の形態では、媒体34は外部記憶装置12以外の装置からはアクセス不可能になるが、LCを複数書き込み可能な媒体を用いれば、それを複数の装置からアクセス可能にすることもできる。

【0042】図8は、複数のLCを持つ媒体を示している。図8の媒体41は、MIDを記憶するMID領域42と、n個(nは1以上の整数)のLCに相当するLC(1)、LC(2)、・・・、LC(n)を記憶するLC領域43とを有する。これらのLC(i)(i=1, 2, ..., n)にはあらかじめSGCが書き込まれているが、各々のSGCをJCへ書き換えることにより、最大n個の異なるDIDを持つ装置を登録することができる。

【0043】図9および図10は、媒体41へのアクセスの可否を判定する第2のアクセス判定処理のフローチャートである。図9において処理が開始されると、処理部13は、まずDID記憶部33からDIDを読み出し(ステップS41)、制御変数iを1とおく(ステップS42)。

【0044】次に、媒体41からMIDとLC(i)を読み出し(ステップS43)、第1の記号生成アルゴリズムに従ってMIDとDIDからJCを作成して(ステップS44)、それをLC(i)と比較する(ステップS45)。作成したJCが媒体41のLC(i)と一致すれば、外部記憶装置12による媒体41へのアクセスが可能と判定し(ステップS46)、処理を終了する。

【0045】ステップS45においてJCがLC(i)と一致しなかった場合は、iをnと比較する(ステップS47)。そして、iがnより小さければi=i+1とにおいて(ステップS48)、ステップS43以降の処理を繰り返す。

【0046】ステップS47においてiがnに達すると、JCはいずれのLC(i)とも一致しなかったことが分かる。そこで、次に、第2の記号生成アルゴリズムに従ってMIDからSGCを作成し(図10、ステップS49)、再びi=1とおく(ステップS50)。

【0047】次に、作成したSGCをLC(i)と比較し(ステップS51)、SGCがLCと一致すれば、媒体41上のLC(i)をJCに置き換え(ステップS52)、図9のステップS42以降の処理を繰り返す。ステップS51においてSGCとLC(i)が一致しなかった場合は、iをnと比較する(ステップS53)。そして、iがnより小さければi=i+1とにおいて(ステップS54)、ステップS51以降の処理を繰り返す。

【0048】ステップS53においてiがnに達すると、いずれのLC(i)にもSGCが格納されておらず、新たな装置の登録は不可能であることが分かる。そこで、外部記憶装置12による媒体41へのアクセスは不可能と判定し(ステップS55)、処理を終了する。

10

20

30

40

50

【0049】このような第2のアクセス判定処理によれば、最大nまでの外部記憶装置に対して、媒体へのアクセスを許可することが可能になる。第1および第2のアクセス判定処理において、MIDを用いて生成される初期のLCの例として供給者が作成するSGCを挙げたが、これ以外に、媒体の所有者が独自に作成した特殊記号（SPC：special code）を用いることもできる。

【0050】この場合、媒体の所有者は、そのLC領域のSGCをあらかじめユニークに決定されたSPCに書き換えておき、その生成アルゴリズムを第2の記号生成アルゴリズムとして、PC11からRAM24内にロードしておく。そして、処理部13は、図7のステップS36や図10のステップS49において、そのアルゴリズムを用いてSPCを作成し、ステップS37やステップS45において、SPCをLCやLC(i)と比較する。

【0051】このようにSGCの代わりにSPCを用いれば、その生成アルゴリズムは、媒体の供給者を含めて所有者以外の誰も知らないことになる。したがって、装置が未登録の状態でも、所有者以外の装置は媒体にアクセスすることができなくなる。特に、媒体と装置とをシステムの統合して運用する組織、例えば銀行においては、このようなSPCを書き込んでおくことが有効である。この場合、SPCは、その組織の責任の元に決定され、使用される。

【0052】ところで、アクセス判定のアルゴリズムは上述したようにRAM24内に格納されており、必要に応じてその1部または全部を変更することが可能である。例えば、第1のアクセス判定処理において、JCを作成する第1の記号生成アルゴリズムがRAM24内で変更された場合、そのままでは媒体34への以後のアクセスが不可能になる。そこで、アルゴリズムの変更を検出する処理が必要になる。

【0053】図11は、このような第1の記号生成アルゴリズムの変更に対応可能な第3のアクセス判定処理のフローチャートである。第3のアクセス判定処理の全体フローは、図7の第1のアクセス判定処理のフローに図11の3つのステップを挿入して得られる。

【0054】図7のステップS34においてJCがLCと一致しなかった場合、処理部13は、次に第1の記号生成アルゴリズムが変更されたかどうかを調べる（ステップS61）。第1の記号生成アルゴリズムが変更されていないければステップS36以降の処理に進み、媒体34が新しいかどうかを調べる。

【0055】それが変更されている場合は、変更前の記号生成アルゴリズムに従ってMIDとDIDからJC'を作成し（ステップS62）、それをLCと比較する（ステップS63）。変更前の記号生成アルゴリズムは、その変更時に、旧アルゴリズムとしてRAM24内に残されているものとする。

【0056】ここで、作成したJC'がLCと一致しなければステップS36以降の処理に進み、媒体34が新しいかどうかを調べる。両者が一致すれば、媒体34に外部記憶装置12が登録されていたことが分かるので、ステップS38の処理に進み、LCを変更後のアルゴリズムにより作成されたJCに置き換える。こうして、新しいアルゴリズムを用いて外部記憶装置12が再登録される。

【0057】以上の実施形態においては、外部記憶装置の処理部がRAMに格納されたプログラムを用いて、復号処理やアクセス判定処理等の、媒体内の情報のセキュリティ保護に関する処理を行っている。このようなセキュリティに関する他の処理として、媒体内のデータの暗号化処理、コード変換処理、データ修飾処理等を行うことも可能である。さらに、処理部は、媒体とPCの間でやり取りされる情報のより一般的な加工処理を行うこともできる。

【0058】

【発明の効果】本発明によれば、外部記憶装置の処理部に書き換え可能な領域を設けたことで、その処理プログラムがロードブルになり、装着された媒体内の情報のセキュリティ保護をフレキシブルに行うことができる。例えば、データと対して媒体内に記憶されたプログラムをロードして、そのデータへのアクセスに関する処理を行うことができる。これにより、データ毎にまたは媒体毎に異なる暗号化アルゴリズムを採用することが可能になる。

【0059】また、許諾された記憶媒体と記憶装置の対においてのみ、媒体の記憶内容へのアクセスを許可することが可能になり、過失、故意によって形成された他の対におけるデータへの不正なアクセスを禁止することができる。

【0060】したがって、媒体内の情報のセキュリティや、その情報に関する著作権の保護等が効率的に保証される。

【図面の簡単な説明】

【図1】本発明の原理図である。

【図2】実施形態の構成図である。

【図3】処理部の動作フローチャートである。

【図4】媒体判別処理のフローチャートである。

【図5】復号処理のフローチャートである。

【図6】アクセス判定を行うシステムの構成図である。

【図7】第1のアクセス判定処理のフローチャートである。

【図8】複数のLCを持つ媒体を示す図である。

【図9】第2のアクセス判定処理のフローチャート（その1）である。

【図10】第2のアクセス判定処理のフローチャート（その2）である。

【図11】第3のアクセス判定処理のフローチャートで

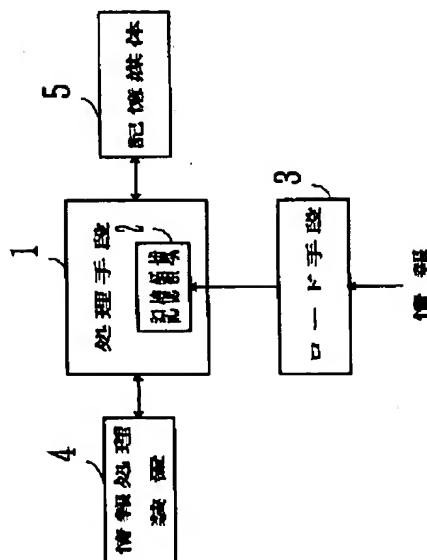
ある。

【符号の説明】

- 1 処理手段
- 2 記憶領域
- 3 ロード手段
- 4 情報処理装置
- 5、15、34、41 記憶媒体
- 11 パーソナルコンピュータ
- 12 外部記憶装置
- 13 処理部
- 14 ヘッド
- 16 データ
- 17 プログラム

【図1】

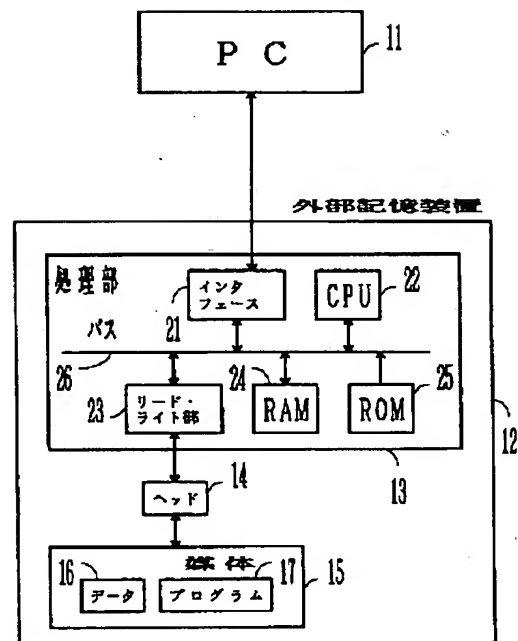
本発明の原理図



- 21 インタフェース
- 22 CPU
- 23 リード・ライト部
- 24 RAM
- 25 ROM
- 26 バス
- 31 アプリケーション・プログラム
- 32 デバイスドライバ
- 33 D I D記憶部
- 35 M I D領域
- 36 L C領域
- 42 M I D領域
- 43 L C領域

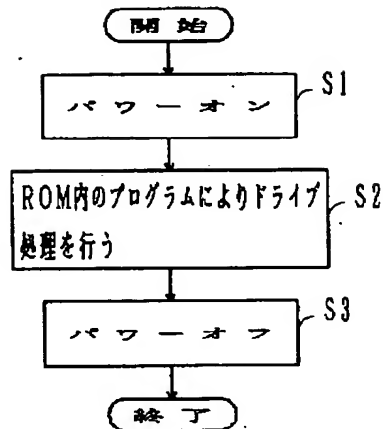
【図2】

実施形態の構成図



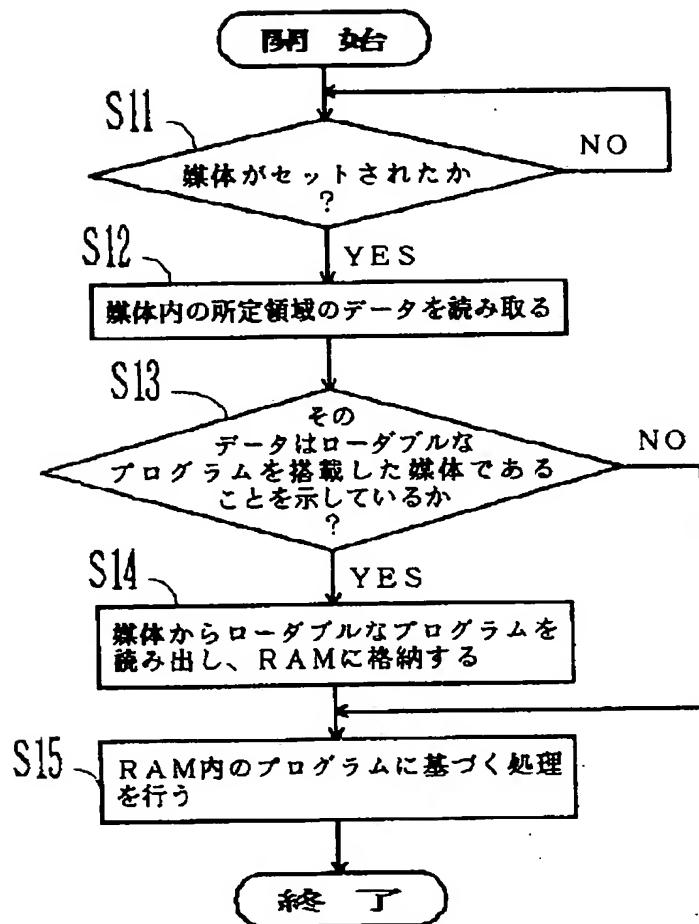
【図3】

処理部の動作フローチャート



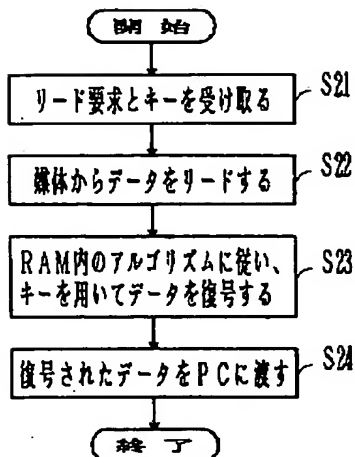
【図4】

媒体判別処理のフローチャート



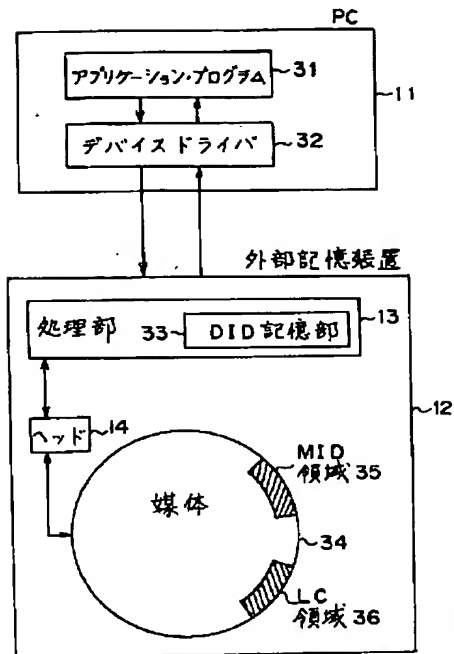
【図5】

復号処理のフローチャート



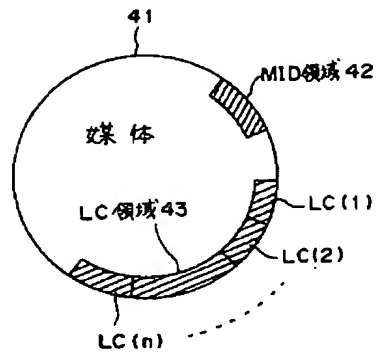
【図6】

アクセス判定を行うシステムの構成図



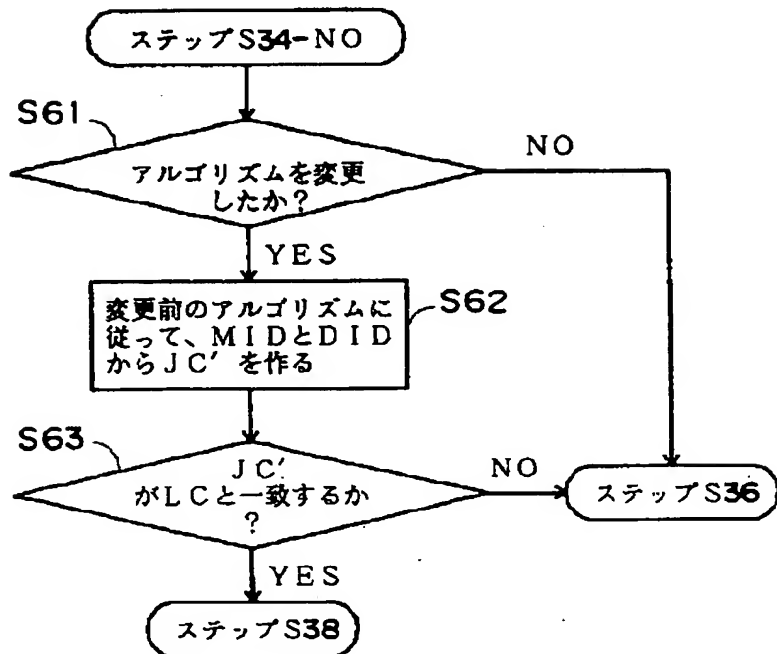
【図8】

複数のLCを持つ媒体を示す図



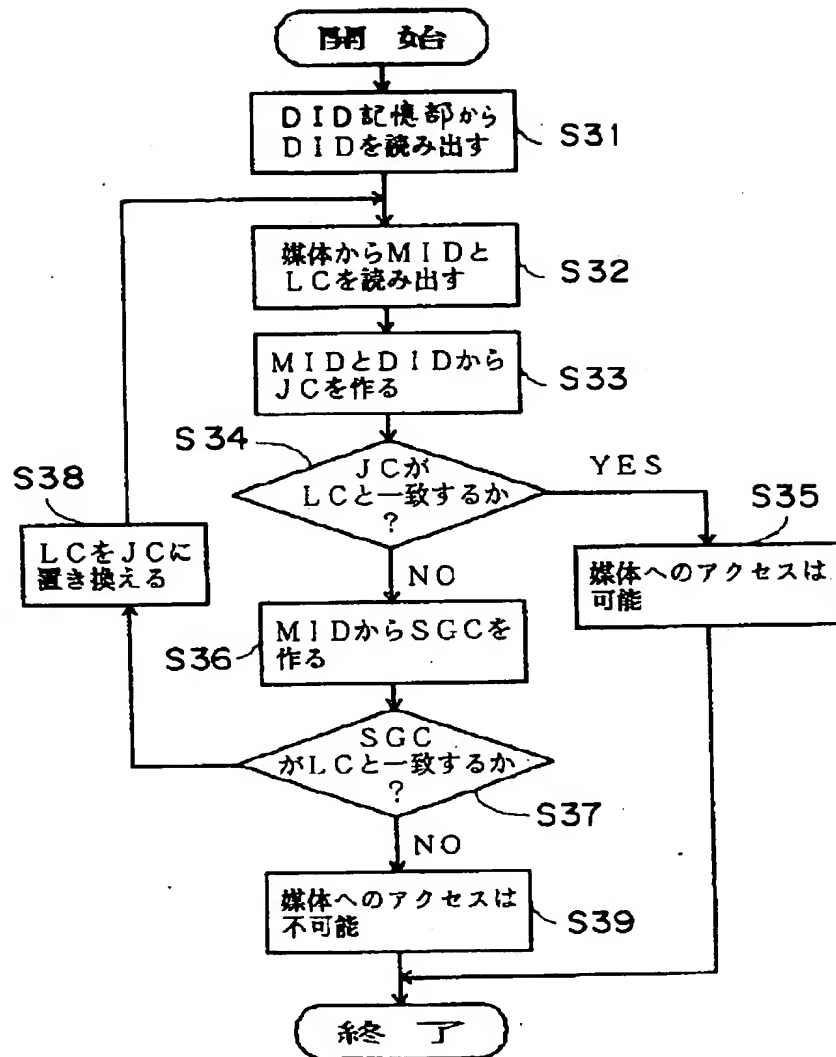
【図11】

第3のアクセス判定処理のフローチャート



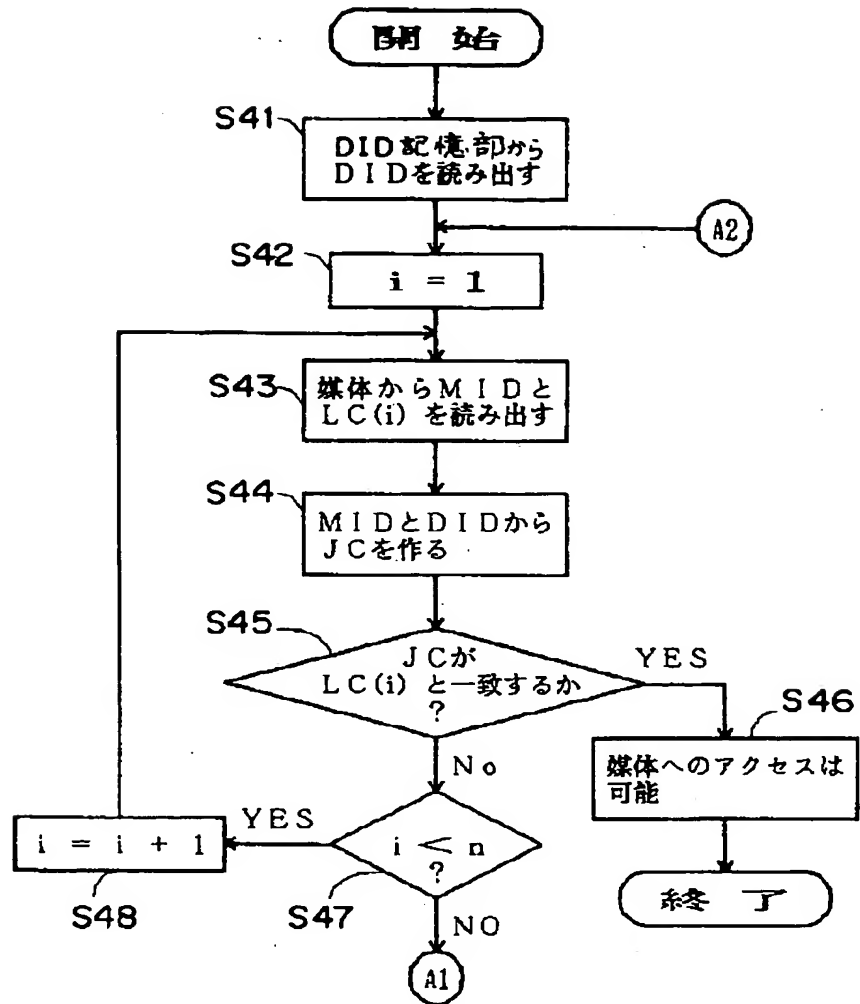
【図7】

第1のアクセス判定処理のフローチャート



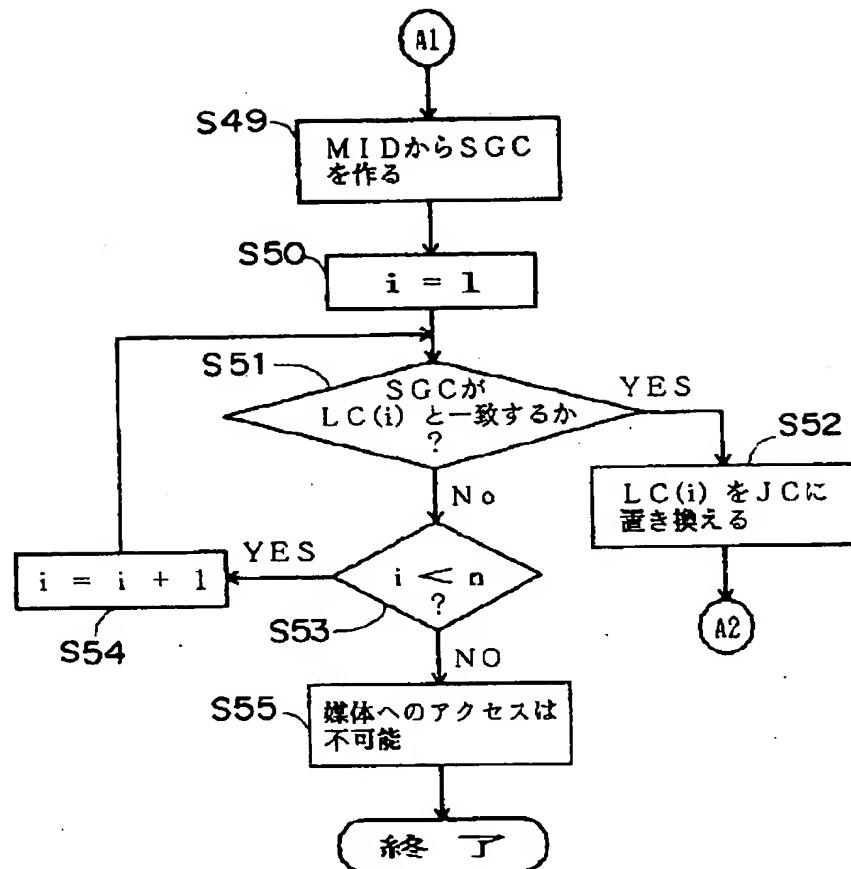
【図9】

第2のアクセス判定処理のフローチャート (その1)



【図10】

第2のアクセス判定処理のフローチャート(その2)



フロントページの続き

(72)発明者 吉本 真一
 神奈川県川崎市中原区上小田中1015番地
 富士通株式会社内

(72)発明者 金元 浩一
 群馬県前橋市問屋町1丁目8番3号 株式
 会社富士通ターミナルシステムズ内

(72)発明者 増田 達朗
 群馬県前橋市問屋町1丁目8番3号 株式
 会社富士通ターミナルシステムズ内

(72)発明者 吉岡 誠
 神奈川県川崎市中原区上小田中1015番地
 富士通株式会社内

(72)発明者 藤原 真雄
 神奈川県川崎市中原区上小田中1015番地
 富士通株式会社内